RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: LAB2-R01

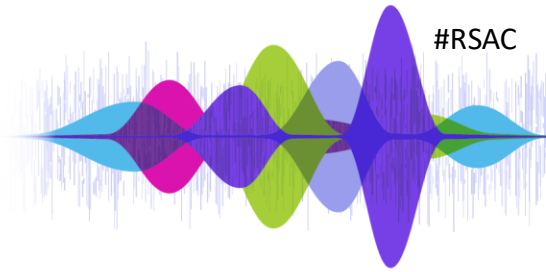
Ransomware from ATT&CK to Zcash: An Interactive Simulation

Harry Halikias

Sr. Director, Global Information Security
https://linkedin.com/in/harryhalikias

Nadean Tanner

Head of ThreatSpace, Mandiant - Google Cloud
Technical Director, Mandiant Cybersecurity
https://linkedin.com/in/nadeanhtanner/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Views expressed are our own and do not represent those of any other people or organizations.

We are not lawyers. Seek qualified legal advice.

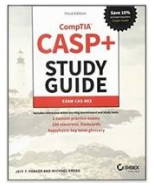
Harry Halikias

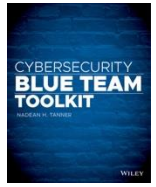
- MCS, CISSP, CIPP/US, SSCP, GSEC, FAIR, CCNA Cyber Ops, S+, N+, A+, ITIL v3, CCP, PSM, PSPO
- Presentation based on grad school research
- Author: Digital Shakedown: The Complete Guide to Understanding and Combatting Ransomware

BROWN

Nadean Tanner

- Head of Threatspace – Google Cloud
- CISSP, CASP+, Metasploit Pro, CTT+, S+, N+, A+, Server+, ITIL v3, CCP, AVM
- Author: Sybex CASP+ Study Guide, Cybersecurity Blue Team Toolkit



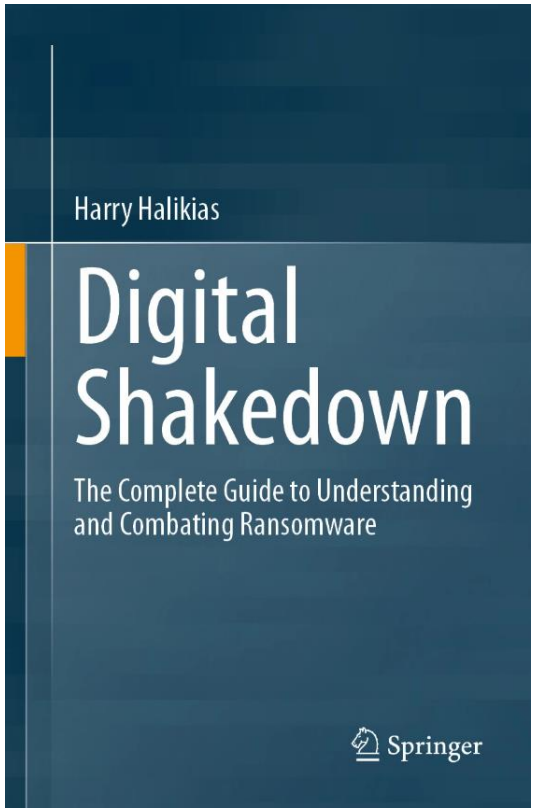


What to expect

- Learn about
  - Ransomware and extortion attacks
  - How attackers pressure victims
  - Tabletop exercises
- Think about how you would respond. Who takes what action?
- Consider different perspectives
- Ask stupid questions
- Have fun, make friends, share knowledge

The Paper

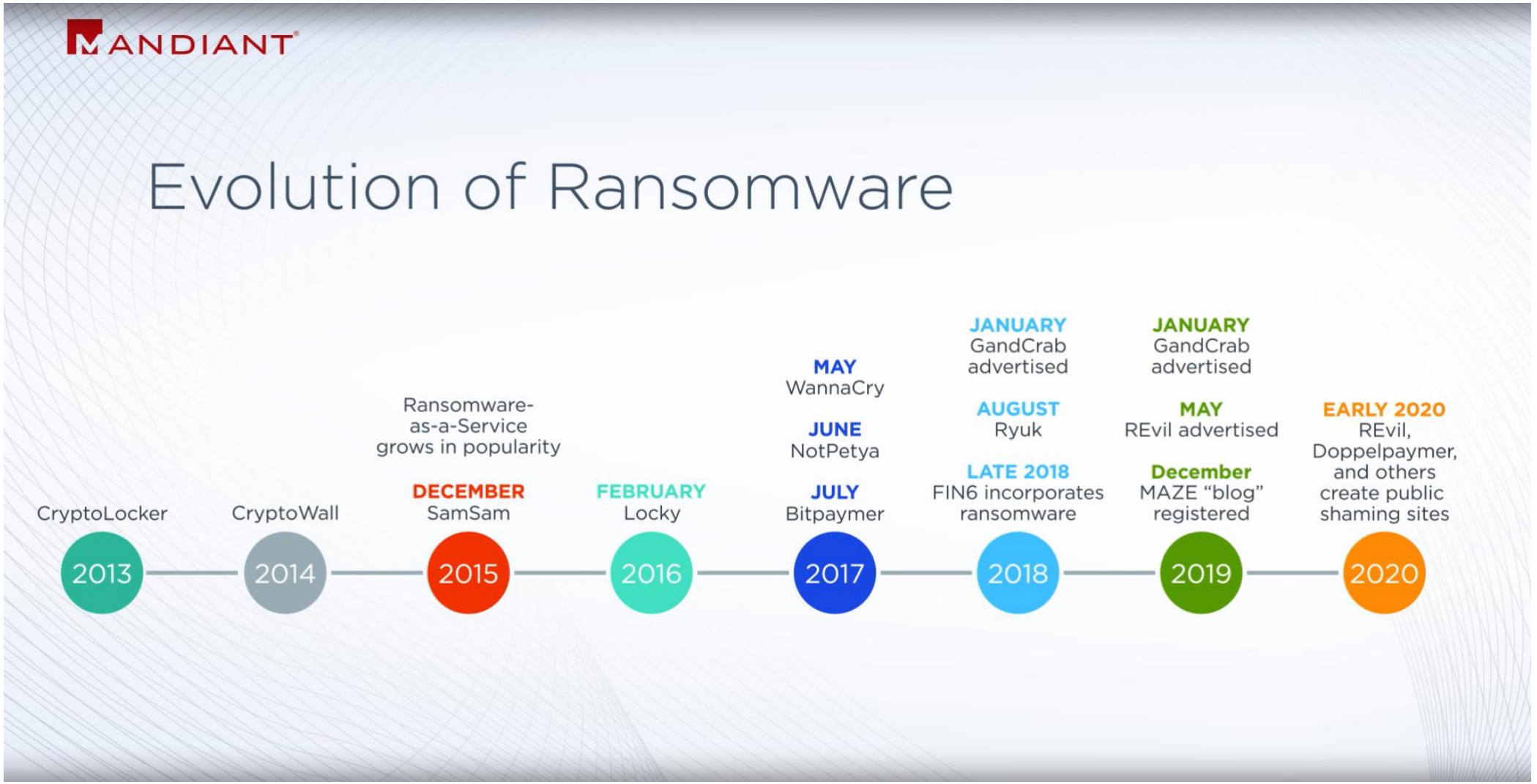
- Comprehensive academic research on ransomware
- Three C's of Ransomware
  - Cryptography
  - Cryptocurrency
  - Customer Service
- Business Impacts
- Laws and Regulations
- Preparation, Response, and Recovery
- Proposed solutions



What is Ransomware

- Human controlled malicious program that locks files or computers, typically via encryption, and then demands the system owner pay to regain access.
- Some recent breaches used exfiltration and extortion, without encryption.

History of Ransomware



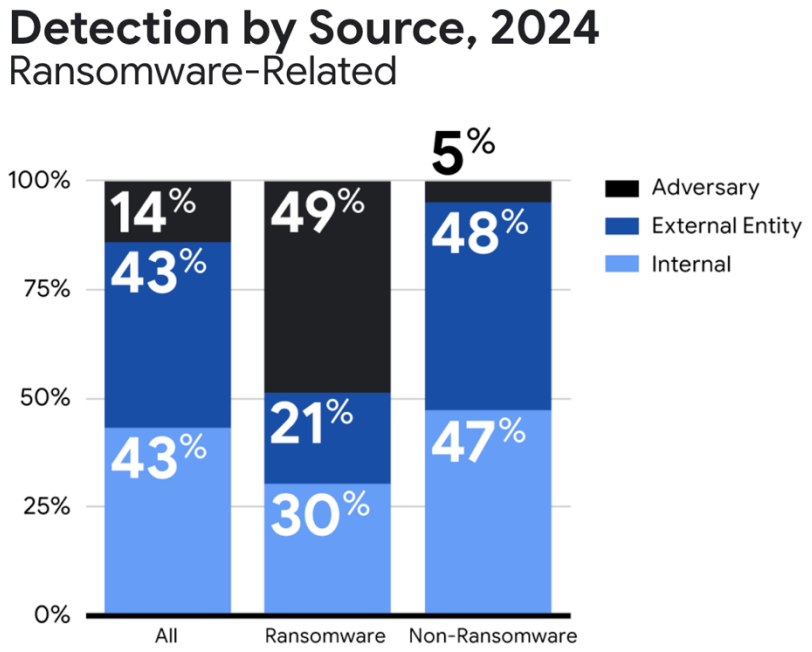
Recent Statistics

- Ransomware attacks increased by 15% in 2024
- 59% of organizations were hit with ransomware in 2024 and ransom bills increased 500%.
- 2021 CISA: Ransomware impacted 14 of 16 Critical Infrastructure Sectors

www.gov.il/BlobFolder/reports/alert_1863/he/ALERT-CERT-IL-W-1863.pdf
https://www.sophos.com/en-us/content/state-of-ransomware
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a

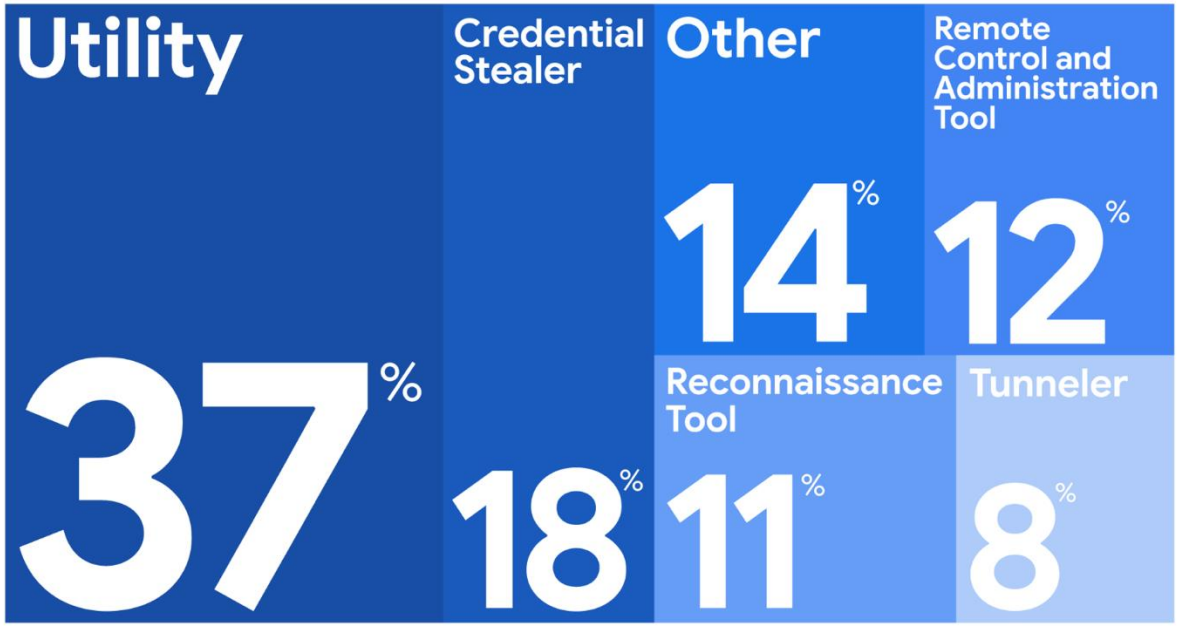
Ransomware-Detection by Source

This is consistent with the extortion business model in which attackers intentionally and abruptly notify organizations of a ransomware intrusion and demand payment.

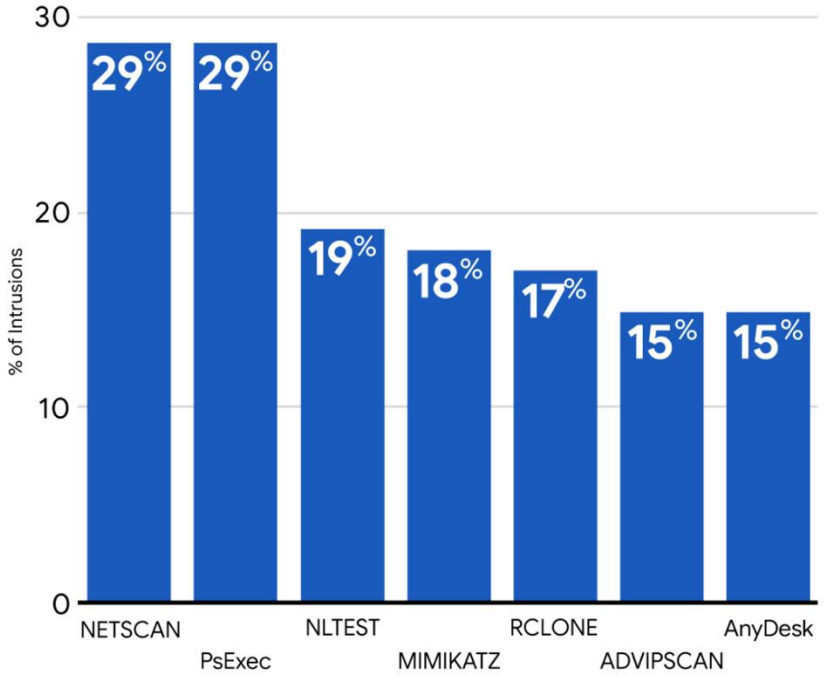


Observed Tools

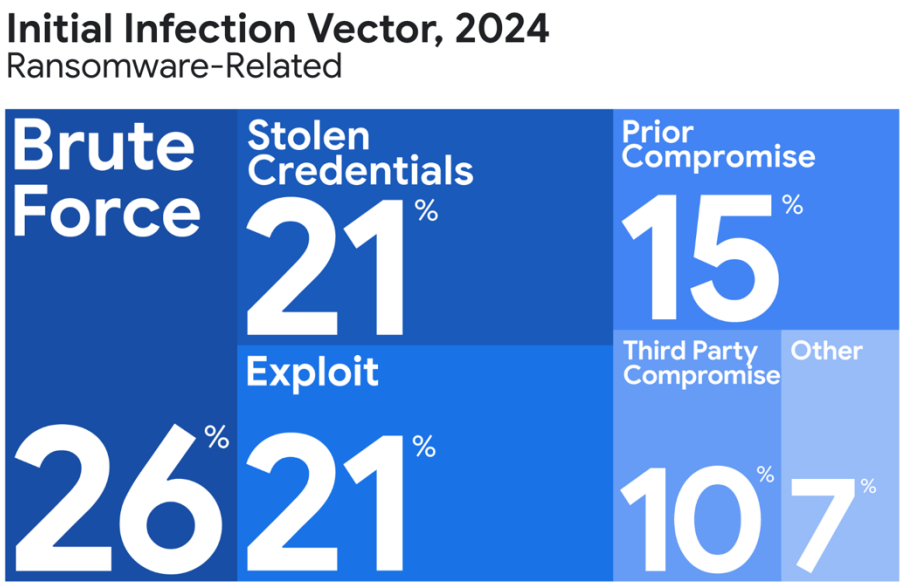
Observed Tools, 2024
Ransomware-Related

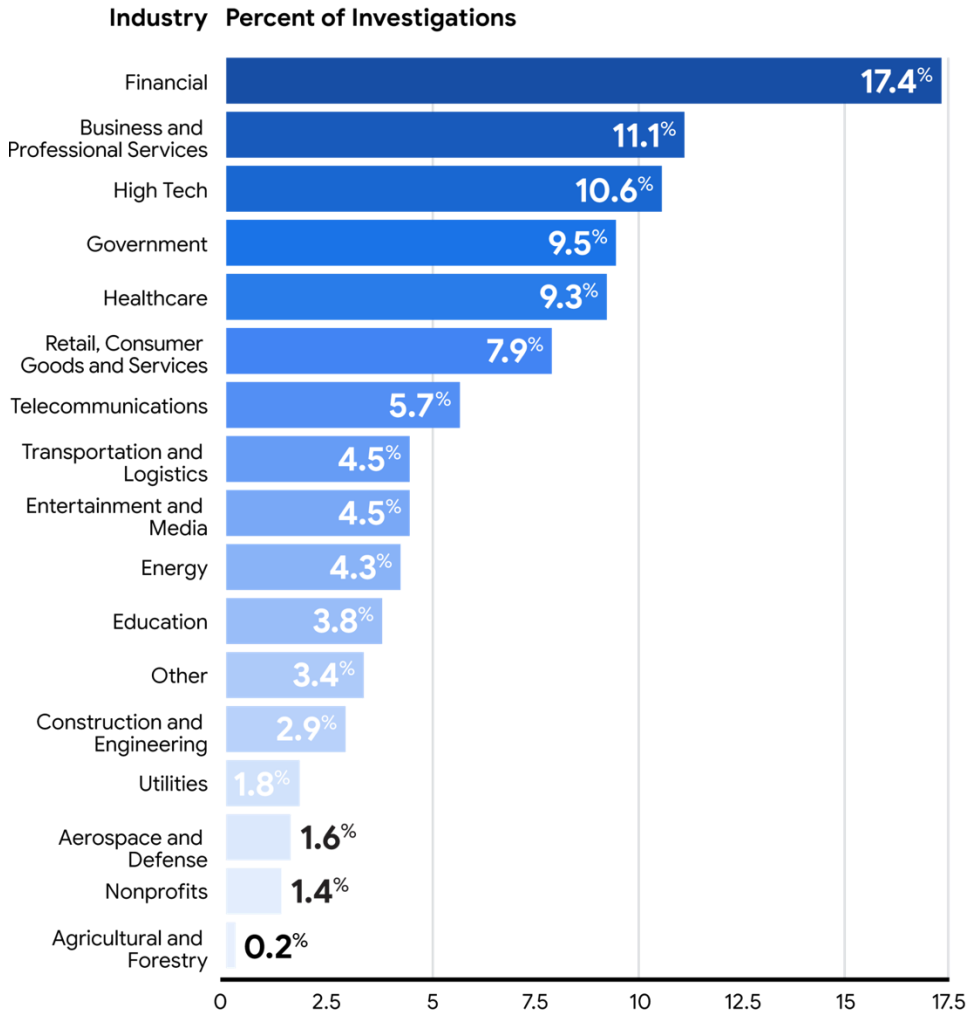


Most Frequently Seen Tools, 2024
Ransomware-Related



Ransomware-related Intrusions



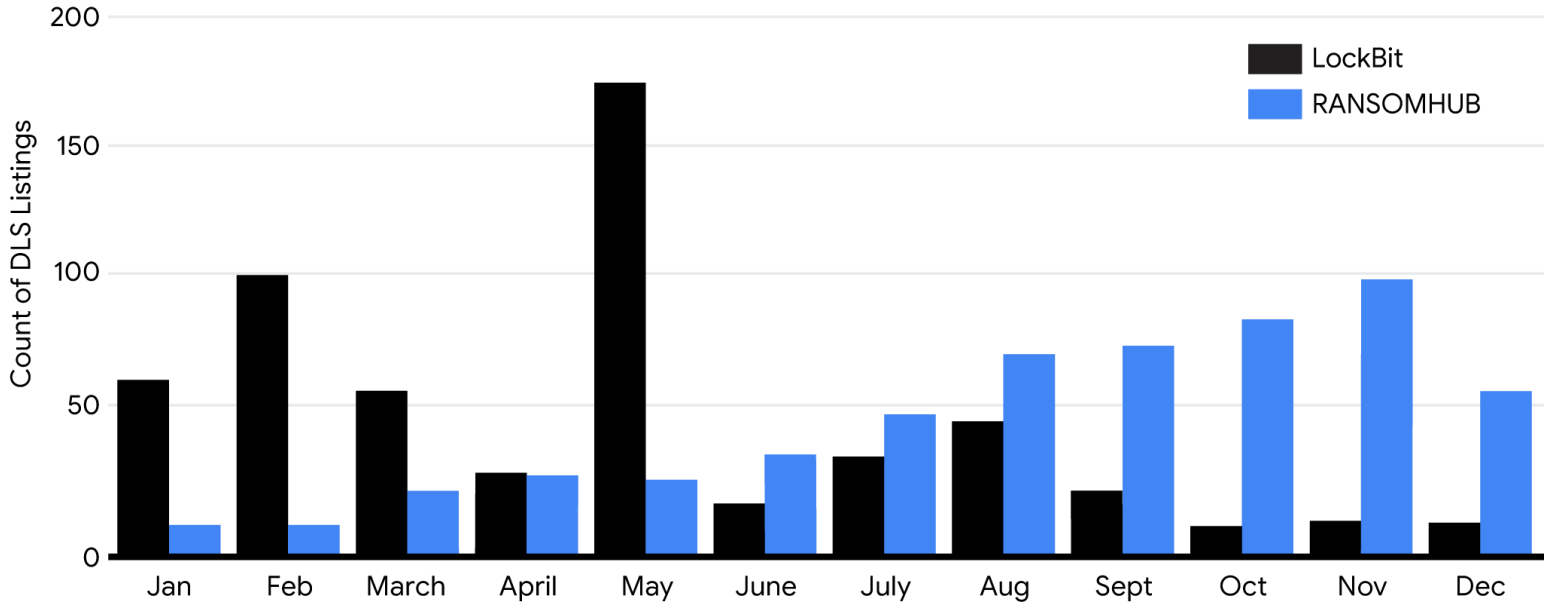


Ransomware Operations

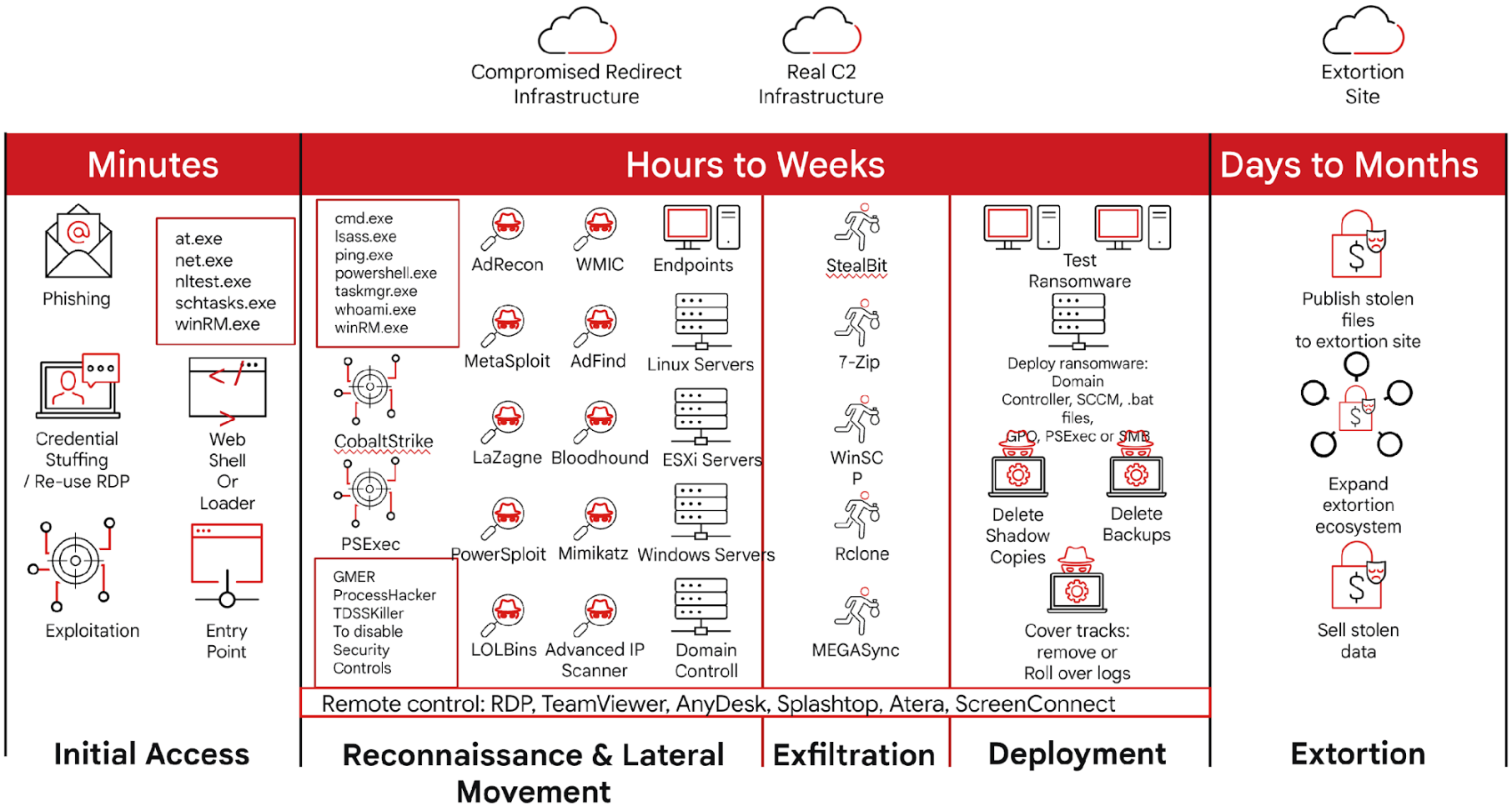
By the second half of 2024, RANSOMHUB RaaS became the most prolific DLS that Mandiant tracks, taking the top spot from LockBit after its activity declined following law enforcement action

LockBit vs. RANSOMHUB DLS Listings, 2024

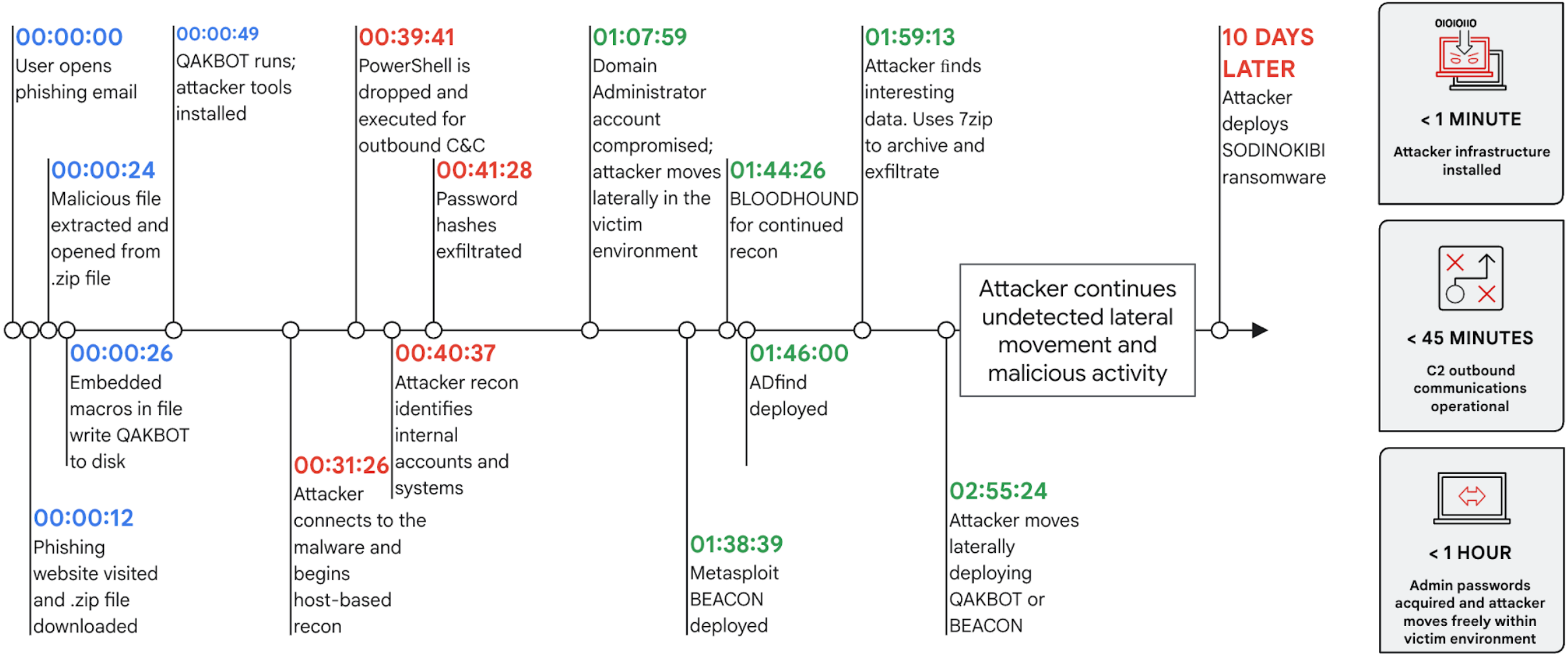
Ransomware-Related



Ransomware Lifecycle



What does a ransomware attack look like?



Tip: CISA Ransomware Vulnerability Warning Pilot

- RVWP
- CIRCIA Requirement
- Proactive notification by CISA
- Part of CISA Cyber Hygiene Vulnerability Scanning
- No separate sign up

https://www.cisa.gov/stopransomware/Ransomware-Vulnerability-Warning-Pilot

Interactive Simulation

- Tabletop style
- Pose a scenario
- Pick the best option

- Yes, we have insurance

Practice: What is the best food in San Francisco?

- Sourdough bread
- Cioppino
- Mission Burrito
- Fortune cookies

What is the motivation of ransomware?

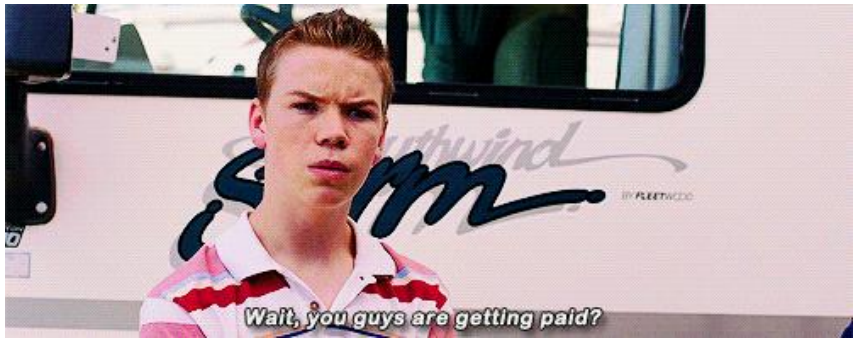
- Destroy Data
- Get Paid
- Sometime both

Answer: Sometimes both

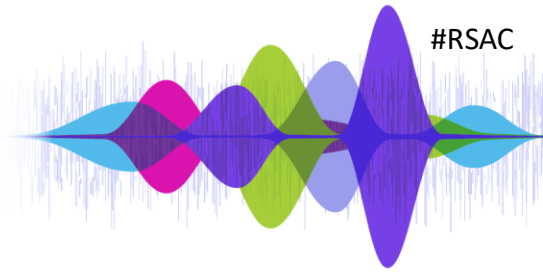
Why?

Fear and pressure

- Primary purpose is payment
- Ransomware promises a path to recovery, real or not
- They have something you want.
  - A way to recover your data or prevent it from leaking

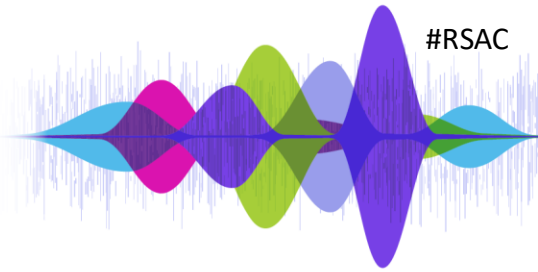


Cybersecurity Analyst at MSF Hospital System



- Small team
- 12 Hospitals
- 4,235 Beds in the hospital system with a 79.7% usage rate

Sampled from: https://council.nyc.gov/budget/wp-content/uploads/sites/54/2019/02/Health-and-Hospitals-Hospital-Utilization-Report.pdf



Scenario

- Thursday, May 1, 2025
  - Complaints about network performance
- Friday 4:45 PM
  - Alerts for files with unusual extensions
  - Alerts about new processes
  - Help desk receives calls about files not opening
  - Received text message from your friend Duane in accounting with a picture

readme ×

Hello!

If you are reading this, it means that your system were hit by Royal ransomware.
Please contact us via :
http://[redacted]asdfdfdfdfddfdfdfdfdfffffffffffd

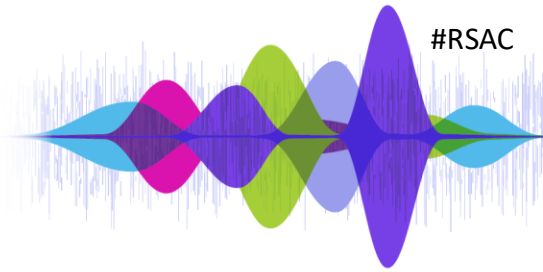
In the meantime, let us explain this case.It may seem complicated, but it is not!
Most likely what happened was that you decided to save some money on your security infrastructure.
Alas, as a result your critical data was not only encrypted but also copied from your systems on a secure server.
From there it can be published online.Then anyone on the internet from darknet criminals, ACLU journalists, Chinese government(different names for the same thing),
and even your employees will be able to see your internal documentation: personal data, HR reviews, internal lawsuitsand complains, financial reports, accounting, intellectual property, and more!

Fortunately we got you covered!

Royal offers you a unique deal.For a modest royalty(got it; got it ?) for our pentesting services we will not only provide you with an amazing risk mitigation service,
covering you from reputational, legal, financial, regulatory, and insurance risks, but will also provide you with a security review for your systems.
To put it simply, your files will be decrypted, your data restoredand kept confidential, and your systems will remain secure.

Try Royal today and enter the new era of data security!
We are looking to hearing from you soon!

Source: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-royal
Also check out ransom note at: https://www.group-ib.com/blog/ransomhub-raas/



What do we know?

- Ransom notes appeared
- Files are inaccessible
- Don’t know how many machines
- Calls are coming in

Scenario 1: What do we do?

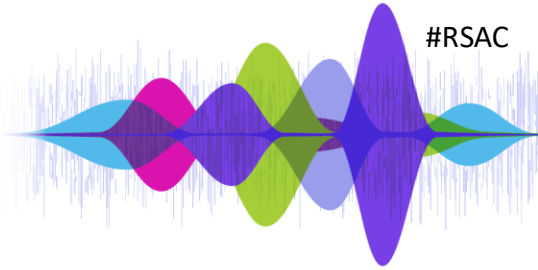
a. Report the incident to law enforcement and notify hospital leadership

b. Attempt to identify and isolate the affected systems

c. Pay the ransom immediately to avoid potential service disruptions

d. Consult the incident response plan

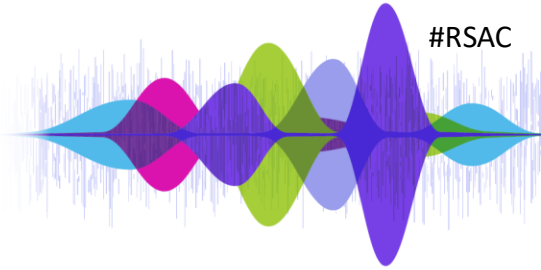
Consult the Incident Response Plan



- Good news: You have an incident response plan similar to 95% of organizations
- Bad news: It doesn’t cover ransomware similar to 13% of organizations
- Worse news: The IR Plan is on the file server and has a fancy new extension Incident_Response_Plan.pdf.c39dk20

Source: H. Halikias, *Digital shakedown*. 2024. doi: 10.1007/978-3-031-65438-1.

Scenario 2: System Impact Assessment



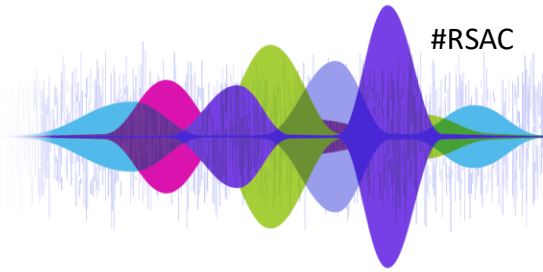
The IT department identifies that the ransomware has encrypted critical patient data and Electronic Health Record (EHR) systems, affecting multiple hospitals within the network.

a. Continue efforts to identify and isolate the affected systems and activate the Incident Response Team

b. Activate the hospital's business continuity and disaster recovery plans

c. Notify all staff members about the incident and instruct them on how to proceed

Scenario 3: How should we contain the incident?



a. Ask users to shut down computers
b. Ask users to hibernate computers
c. Ask users to disconnect the network cable
d. Disconnect the entire network
e. Use tools to take the network offline or disrupt communications

Answer: e. Use tools to take the network offline or disrupt communication

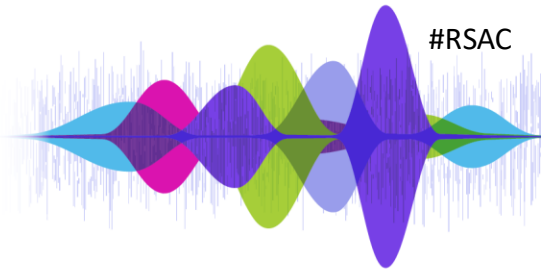
The Great Shut Down, Reboot, Pull the Plug debate

CISA	"Take Network offline at switch level." If not possible, "power down to avoid further spread."
EMSISOFT	"Do not restart impacted devices." "Impacted systems should be put into hibernation."
FTC	"Immediately disconnect the infected computers or devices from the network."
IBM	"Do not reboot or restart an infected system." "The infected system should be hibernated and disconnected from the network immediately." "Shut down immediately" if encryption has begun but not completed (no ransom note displayed).
Justice Department	"Remove from the network as soon as possible." "Isolate or power-off affected devices that have not yet been completely corrupted."
Secret Service	"Do not power down or shutoff any systems affected by ransomware."

Table 11: Advice on whether to restart an infected computer during a ransomware incident.

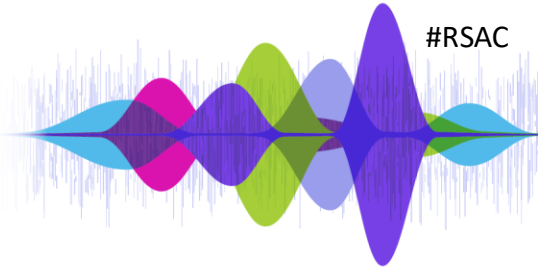
Source: H. Halikias, *Digital shakedown*. 2024. doi: 10.1007/978-3-031-65438-1.

Who gives the order? Who takes action?



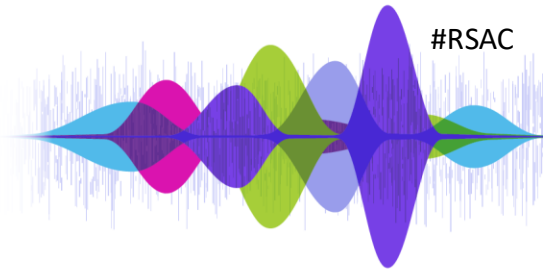
- Practical problems with shutdowns, cable pulling, hibernation, etc.
  - Who communicates it?
  - How is it communicated?
  - What about WiFi?
  - How many core switches are there?
  - Will it destroy evidence?
  - Who takes the action? Do you need a network engineer outside of security?
  - Does it need approval?

Automated and pre-configured tools



- Can recognize signs of attack
  - Known IOC's
  - Unusual extensions
  - Unusual encryption activity
  - Unusual peer communication
- Detects and automatically blocks or alerts

How do we Activate the Incident Response Team?



- Do we trust our communication systems?
- Contact info was in email
- Systems are clearly compromised

Tip: Use an out of band crisis management system

- BC, DR, and Recovery info
- Contact info
- Insurance info
- Leadership info
- Communications templates
- OOB Communications

- HR sometimes has these systems
- Consider keeping the system a secret

In Case of Crisis by RockDove Solutions

ONSOLVE SEND WORD NOW

EVERBRIDGE CRISIS MANAGEMENT

slack

Signal

Email sent to CEO, CISO, CIO, General Counsel

Your network has been hacked Inbox ×

Ransomware Customer Service <mnyppay1750@protonmail.com>
to me

MSF Hospital System

Your network has been hacked and encrypted.

This page and your decryption key will expire in 10 days after your systems were infected.
Sharing this link or email will lead to irreversible removal of the decryption key.

All your files, backups and shadow copies have been encrypted and currently unavailable.

Any attempt to recover your files without the decryption tool leads to the data destruction.
DO NOT RESET/SHUTDOWN - files will be damaged.
DO NOT RENAME/MOVE/DELETE the encrypted and readme files.
DO NOT USE ANY RECOVERY SOFTWARE that is aimed to restore the encrypted files.
Any of the above makes the file recovery impossible.

Also, we have gathered all your private data.
Sensitive information will be disclosed to public or sold to re-seller if you decide not to pay.

The service fee for helping your security is 435 BTC.

The price gets higher as the timer counts down the time.
09 02h:54m:45s 435 BTC

The price you get until timer counts down the time.

It may take us a few hours to reply.

Based on Dopplepaymer

Employees are posting on social media

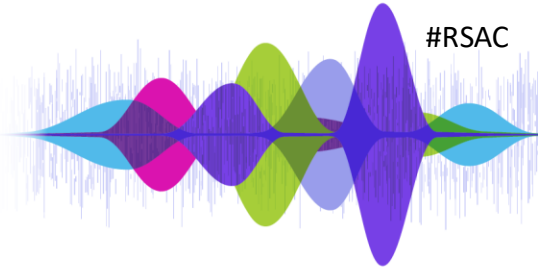
steponeonestep OP · 2 yr. ago · *edited 2 yr. ago*

Medical Student

Starter comment: I'm rotating at a UHS facility and all systems are down right now. We don't have internet or access to charts right now because of this ransomware attack, and there isn't a solid ETA on when we'll get access. Don't know too many details, but I wanted to post to hear some thoughts about this and other critical health systems affected by attacks like this. I know the NHS experienced something similar but it was resolved because of poor coding on the ransomware hacker's part.

Edit: Finally hit national news: https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254

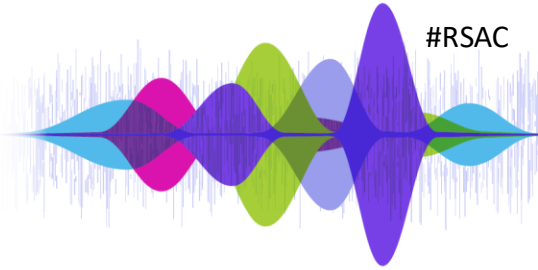
Scenario 4: But wait, there's more!



News outlets have picked up the story, and the hospital is facing intense media scrutiny and public concern over patient privacy.

a. Designate a spokesperson to address the media and provide updates
b. Draft a public statement acknowledging the incident and outlining steps taken to mitigate its impact
c. Refrain from making any public statements until the situation is resolved

External Communication



- FBI/Secret Service/IC3/CISA
  - FBI says call the FBI.
  - Jason Conboy from DHS says “call anybody”
- Insurance Company
- Outside Counsel
- Customers
- Suppliers
- Regulators (US Dept. Of Health, SEC, FTC, NY DFS, California AG, Supervisory Authority, etc.)
- Media

Who makes the decision to contact external parties?

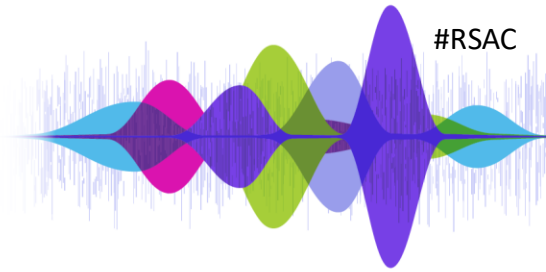
a. CEO/President
b. CISO
c. Legal
d. CFO
e. Corporate Communications
f. Incident Commander
g. Other
h. Don’t know

Tip

“Don’t answer the phone until legal gives you advice”

Hanslovan and Bisnett, hack_it 2020

Scenario 5: Law Enforcement Involvement



The FBI contacts the hospital, informing them that they have been tracking the ransomware group behind the attack and have actionable intelligence on their location.

a. Collaborate with law enforcement, sharing information and following their recommendations

b. Continue to handle the situation internally, while keeping law enforcement informed of any major developments

c. Decline law enforcement assistance, focusing on internal efforts to resolve the incident

d. Use intelligence gained from the investigation to launch a counterattack against the threat actors to disrupt their operations and delete stolen data

No Hacking Back but…

- Microsoft and Fortra received a court order to seize domains and take down IP addresses hosting cracked Cobalt Strike (4/13/23)

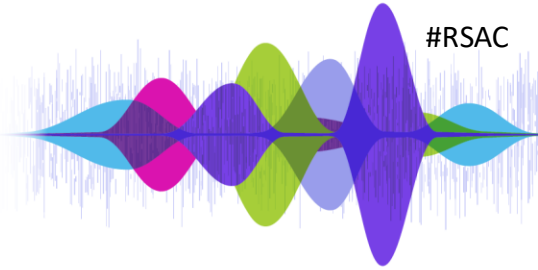
Article: https://www.bleepingcomputer.com/news/security/microsoft-and-fortra-crack-down-on-malicious-cobalt-strike-servers/

Court order: https://www.documentcloud.org/documents/23745706-microsoft-cobalt-strike-court-order

Latest Update

- Ransom notes visible and sent to leadership
- $40 Million Ransom Demand due in 10 days
- Hospital services impacted
  - Non-emergency appointments cancelled but no efficient way to contact patients
  - Deferred Emergency Room Patients
  - Systems with patient and payment information are down
  - Out of Band Comms activated for InfoSec and Leadership
- IT
  - 8-30 days to recover for healthcare environments (Sophos Insights)
  - Have backups. Not confident in integrity of restore locations
  - Haven’t determined if backups are clean

Scenario 6: Should we pay the ransom?



a. Yes, pay $40 Million

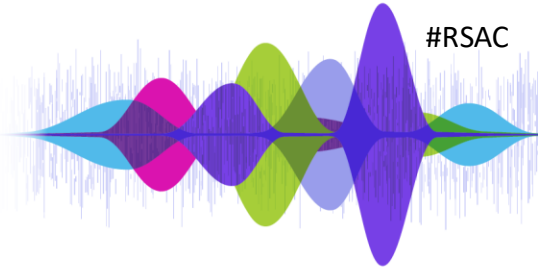
b. Negotiate for more time and a lower ransom

c. No, do not pay the ransom

It’s a business decision

- What is the cost of downtime?
- What percent of critical services can be restored in a certain timeframe?
- Is “betterment” preferred over recovery?

But we have backups!



- Ransomware gangs pivoted to extortion and shaming in 2019
- Companies paying to avoid disclosure
- Blackbaud paid a ransom even though files WEREN'T encrypted

Source: https://www.zdnet.com/article/cloud-provider-stopped-ransomware-attack-but-had-to-pay-ransom-demand-anyway/

Who is the final decision maker on paying ransoms?

- Designated leader (CEO/President) based on input from their team, Board, insurance, and law enforcement
- Not the
  - General Counsel
  - Privacy Officer
  - CISO
  - CFO
  - CIO

Insurance Update

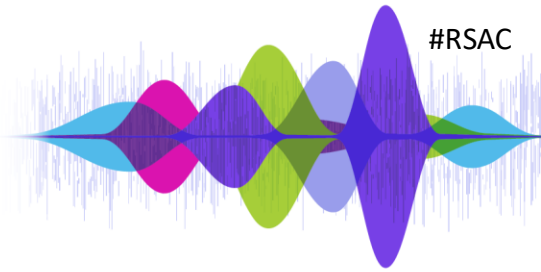
- Insurance assigned a negotiator
- Negotiated ransom reduction if $4 Million Paid immediately
  - New Ransom: $35 Million paid in 12 days
  - Promises no more negotiations

Law Enforcement Update

- Law enforcement discovers that an employee has teamed up with cybercriminals to target the hospital system.

Based on: https://www.bbc.com/news/world-us-canada-56469475
https://www.wired.com/story/tesla-ransomware-insider-hack-attempt

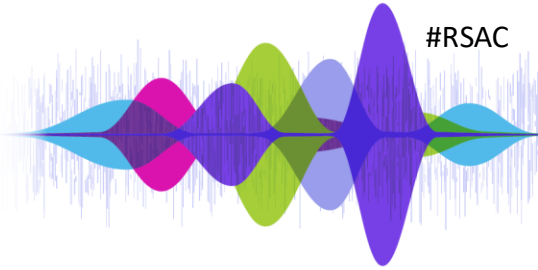
Scenario 7: Should we pay the ransom?



a. Yes, pay $35 Million

b. No, do not pay the ransom. (8-30 day recovery window)

What does leadership need to know?



- What happened?
- How did it happen?
- What is working and what isn't?
- What are required to do by law and by contract?
- How do we minimize legal liability to 3rd parties and customers?
- Public disclosure requirements (Is there a time limit?)
- How much downtime will there be?
- Do we have backups?

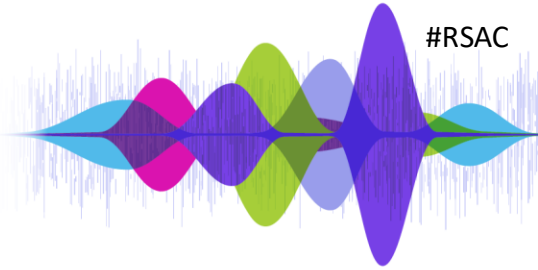
RSA Conference 2022: What To Do When Ransomware Hits: Simulation for CEOs, CISOs and Directors
https://youtu.be/URWrNRjlwiQ

COMMON MITIGATION RECOMMENDATIONS

Address Infection Vectors	• Use enterprise network, email, and host-based security products with up-to-date detections to prevent and detect many common malware strains such as TRICKBOT, DRIDEX, and EMOTET. • Contain and remediate infections quickly to prevent attackers from conducting follow-on activity or selling access to other threat actors for further exploitation. • Perform regular network perimeter and firewall rule audits to identify any systems that have inadvertently been left accessible to the internet. Disable RDP and other protocols to systems where this access is not expressly required. Enable multi-factor authentication where possible, particularly to internet-accessible connections • Enforce multi-factor authentication - do not allow single factor authentication for users who have not set up the multi-factor mechanism.
Implement Best Practices	• Carry out regular anti-phishing training for all employees that operate a device on the company network. • Implement network segmentation to prevent a potential infection from spreading. • Create regular backups of critical data necessary to ensure business continuity and, if possible, store them offsite, as attackers often target backups. • Disallow cleartext passwords to be stored in memory in order to prevent Mimikatz credential harvesting • Consider cyber insurance that covers ransomware infection.
Establish Emergency Plans	• Ensure that after-hours coverage is available to respond within a set time period in the case of an emergency. • Institute after-hours emergency escalation plans that include redundant means to contact multiple stakeholders within the organization and 24-hour emergency contact information for any relevant third-party vendors.

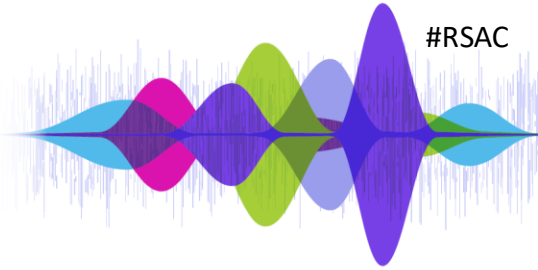
©2021 Mandiant

Apply What You Have Learned Today



- Next week you should:
  - Define criteria for critical assets
  - Locate cyber insurance policy and find out how ransomware is covered and what services are included (ransom negotiators, public relations, forensics, legal, etc.)
  - Watch “What To Do When Ransomware Hits: Simulation for CEOs, CISOs and Directors” https://youtu.be/URWrNRjlwiQ
  - Prepare for meetings with leadership and key partners to understand the impacts of a major ransomware or extortion attack
- In the first three months following this presentation you should:
  - Plan tabletop exercises with different groups simulating the response to an incident (executives, IT, supply chain partners)
  - Collect threat intel on ransomware in your industry and region
  - Meet with leadership and key partners. Identify critical assets, processes, systems, data, personnel, and partners based on previously defined criteria
  - Sign up for RVWP (Critical infrastructure orgs)

Apply What You Have Learned Today



- Within six months you should:
  - Implement tabletop exercise report recommendations
  - Implement attack surface management tool and begin fixing things
  - Ensure tool coverage (EDR, VM) on all systems (with proper configs)
  - Test backups AND restores
  - Ensure tool coverage on all systems
  - Review BC and DR plans
  - Train staff on common cyber threats and their impact
- Within twelve months you should:
  - Implement adversary emulation program (Atomic Red Team, MITRE Caldera, Security Validation, etc.) and begin closing gaps
  - Meet with law enforcement partners
  - Create communication templates in collaboration with legal, corporate communications, and PR firm

RSAC 2025 Conference

Many Voices.
One Community.

Harry Halikias
Privacy & Security

Thank You

Let’s connect

OFAC: Unknown if attacker is a sanctioned entity

Question to OFAC: Should an OFAC licensing application be filed when it is unknown that the payment is to a sanctioned entity? What if the person or entity is known to not be on the sanctioned list?

OFAC Response: *Companies can apply for a license if they seek to engage in a transaction/activity that is otherwise prohibited.*

However, as stated in the advisory, license applications will be reviewed by OFAC on a case-by-case basis with a presumption of denial. If the company knows that the transaction/activity does not involve a sanctioned party/jurisdiction, there may not be a reason to contact OFAC unless you have questions or a sanctions nexus is later discovered. However, we recommend that you document how you came to the conclusion that there isn't a sanctions nexus and we still recommend that you work with law enforcement before responding to the ransom attack. Law enforcement will be able to help you determine whether or not you need to contact OFAC.

- *In instances where a sanctions nexus is known, please contact OFAC via this email address, OFAC_Feedback@treasury.gov, and provide us with the following information:*
- *Company or individual name, as well as any other identifying information, for the subject(s) targeted by a ransomware attack or involved in facilitating the ransomware payment; clarify whether any of the foregoing are U.S. persons or otherwise subject to U.S. jurisdiction.*
- *Type of ransomware variant, if available.*
- *Key dates and facts, including the date of attack, date the attack was discovered, ransomware payment deadline, payment instructions, and ransomware payment amount demanded.*
- *An explanation and evidence, if available, of any sanctions nexus.*
- *A statement whether the ransomware attack has been reported to law enforcement, and, if so, which law enforcement entities are aware of the incident.*

Paying ransoms is legal. Paying sanctioned orgs isn't.

ReedSmith
Driving progress
through partnership

Is Paying a Ransom to Stop a Ransomware Attack Illegal?

Authors: Bart W. Huffman, Michael J. Lowell, Wendell J. Bartnick, Julianne K. Nowicki

Cyber extortion has become an attack of choice for some hackers. Hackers have found that extorting organizations may be a better business model than stealing data and trying to sell it on the black market. As more data breaches occur, the value of such data on the black market falls. One type of cyber extortion is ransomware. Ransomware is a form of malware that encrypts data where an organization stores it, and only the attacker has the key to decrypt it. With this attack, an organization still possesses the data; however, the organization is very unlikely to be able to decrypt the data without the hacker's key. So the encrypted data is unusable to the organization without that key. The hacker contacts the organization asking for payment in exchange for the decryption key. If the organization refuses to pay, the data remains encrypted and unusable. If the organization pays, the attacker may provide the decryption key so the organization can recover the data. The sophistication of the malware (and the ransom amounts) has grown tremendously over the past couple of years.

When victimized by a ransomware attack, organizations are faced with many difficult questions, including whether or not to actually pay the ransom. One consideration for answering that question is whether an organization is permitted to pay a ransom under U.S. law.

U.S. Law Generally Does Not Prohibit Paying a Ransom for the Return of People or Goods. U.S. law criminalizes receiving, possessing, or disposing of money that at any time has been delivered as ransom for a kidnapping.[1] There is no generally applicable law prohibiting individuals or organizations from paying ransoms for the return of individuals or goods. However, an important wrinkle to the analysis is that the U.S. government has prohibited any financial transactions (including ransom payments) with certain governments, organizations, and individuals that are on U.S. Sanctions Lists.

Source: https://www.sxsw.com/wp-content/uploads/2018/03/Legality-of-Paying-Ransom-FINAL-2018.1.19.pdf

COMMON RANSOMWARE TYPES AND DEPLOYMENT METHODS

Top Deployment Methods

- PsExec
- Manual
- Installed Service
- Manual via RDP

- Indiscriminate attacks that leverage a self-propagation or worm-like capability to continually redeploy malware.
- Targeted attacks manually executed by criminal organizations and more sophisticated threat actors that typically follow the attack lifecycle and often leverage trusted applications that live in the customer environment to reduce risk of detection (i.e., PSEXEC, Powershell).
- Ideologically motivated attacks with the purpose to cause significant business disruption, but not a deep interest of collecting payment.

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the competent supervisory authority, if there are potential consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, the supervisory authority may consider an investigation to assess compliance with the broader security requirements of Article 32.

Figure 14: GDPR Article 29 Working Party "Examples of personal data breaches and who to notify." Source: (ARTICLE 29 DATA PROTECTION WORKING PARTY 2017)

Ransomhub Ransom note

Hello!

Visit our Blog:

Tor Browser Links:
http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/

Links for normal browser:
http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

>>> If you have an external or cloud backup; what happens if you don’t agree with us?

- All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree with us, information pertaining to your companies and the data of your company’s customers will be published on the internet, and the respective country’s personal data usage authority will be informed. Moreover, confidential data related to your company will be shared with potential competitors through email and social media. You can be sure that you will incur damages far exceeding the amount we are requesting from you should you decide not to agree with us.

>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because the negotiations will make them look incompetent,After the incident report is handed over to the government department, you will be fined <This will be a huge amount,Read more about the GDRP legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward them.And you will not get anything, and except you and your company, the rest of the people will forget what happened!!!!!

>>> How to contact with us?

- Install and run 'Tor Browser' from https://www.torproject.org/download/
- Go to http://an2ce4pqpf2ipvba2djurxi5pnxxhu3uo7ackul6eafcundqtly7bhid.onion/
- Log in using the Client ID:

Source: https://www.group-ib.com/blog/ransomhub-raas/

RSAC™ | 2025 Conference

Many Voices.
One Community.